Legal Constrains for the Protection of Privacy and Personal Data in Electronic Evidence Handling

Pérez Asinari, María Veroníca

Published in:
International Review of Law Computers & Technology

Publication date:
2004

Document Version
Publisher's PDF, also known as Version of record

International Review of Law Computers & Technology, Volume 18, No. 2, Pages 231–250, July 2004

Carfax Publishing
Taylor & Francis Group

Legal Constraints for the Protection of Privacy and Personal Data in Electronic Evidence Handling[1]

MARÍA VERÓNICA PÉREZ ASINARI

ABSTRACT *This paper describes the application of personal data protection rules in the process of e-evidence handling. It focuses mainly on the application of Directive 95/46/EC rules to the digital environment. It also makes reference to the legal risks derived from the collection and processing of e-evidence in violation of privacy and personal data protection law.*

Introduction

Our objective in the CTOSE (Cyber Tools for On-line Search for Evidence) project was to describe the general legal framework and constraints for the protection of privacy and personal data for evidence handling and consider the CTOSE Process Model designed in Work Package 1.[2]

Electronic evidence handling (the way it is captured, analysed, stored, managed and presented for investigation) has to be compliant with European Union (EU), International and National legislation to be admissible in the context of a dispute[3] (*principe de la régularité des preuves*).

Apart from procedural law requirements (applicable in the off-line and on-line worlds), special attention must be paid to the privacy and data protection legal framework. An enormous amount of personal data from Internet users is collected on the Internet by different actors, through different mechanisms.[4] At times the user is aware of this collection[5] and sometimes not. Sometimes this collection (and further processing) is lawful and sometimes not.

In case of a dispute, this data could be constituted as electronic evidence. For this evidence to be admissible it must have been obtained (and processed in general) lawfully. This means that the part of this data that can be considered as 'personal data' must be

Correspondence: Maria Verónica Pérez Asinari, Centre de Recherches Informatique et Droit, 5 Rempart de la Vierge, 5000 Namur, Belgium. E-mail: veronica.perez@fundp.ac.be.

ISSN 1360-0869 print/ISSN 1364-6885 online/04/020231-20 © 2004 Taylor & Francis Ltd
DOI: 10.1080/1360086042000223526

processed (before, during and after the disputed event) in compliance with the applicable legislation protecting it, at national, international and supranational level.

It is important to bear in mind that the subject matter of this paper is mainly a question of fundamental rights. For this reason, it is not possible to make definitive assumptions. Most of the questions that can be formulated in the context of CTOSE dealing with personal data protection have to be analysed from a case-by-case approach, because of the casuistic nature of the topic under study. Moreover, considering that this field of law is embedded in public order principles, final interpretation will always be given by a judge.

In this paper, we will consider Directive 95/46/EC[6] in the light of electronic evidence handling. Further, we will present a brief overview of the legal risks derived from the violation of data protection legislation.

The Running Phase. Scope of Application of Directive 95/46/EC

Deliverable 1.4 of the CTOSE project has defined the 'running phase' of CTOSE process model (CPM) as the normal state of a computer system.[7]

During the running phase data controllers will have to comply with Directive 95/46/EC (its transpositions to national laws) when processing personal data, in general, and electronic evidence (that presents personal data), in particular. In what follows, we will analyse its content.

The delimitation of the scope of application is important in order to attempt to assess questions such as who, for doing what, and where, has to respect the above-mentioned Directive.

Personal Scope of Application

The 'data subject'. The 'data subject' is the person to whom the data relates. Directive 95/46/EC is applicable only to natural persons. Nevertheless, some national laws extend the protection to legal persons (e.g. Italy). Directive 2002/58/EC[8] is applicable to 'the legitimate interests of subscribers who are legal persons'.[9]

The 'data controller'. The 'controller' is the 'natural or legal person, public authority, agency or any other body, which alone or jointly with others, determines the purposes and means of the processing of personal data; [...]'.[10] This is the person who has legal responsibilities *vis-à-vis* the data subject and public authorities. For instance, in the case of a company, it will not be the system administrator, the controller of the personal data processed through the company website, but the director of the company, because he decides the 'purposes and means' of this processing activity. However, it may happen that the system administrator has more autonomy in processing decisions, so this person would be considered the controller.

The 'data processor'. The 'processor' is 'a natural or legal person, public authority, agency or any other body, which processes personal data on behalf of the controller'.[11] A processor does not have direct obligations *vis-à-vis* the data subject. The processor and the persons acting under his authority have a confidentiality obligation.[12] A contract will be necessary between the controller and the processor in order to carry out processing activities.[13]

Material Scope of Application

The Directive is applicable to the 'processing' of 'personal data'.

What are 'processing' activities? Processing of personal data involves 'any operation or set of operations, which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination, blocking, erasure or destruction'.[14]

The collection of personal data on the Internet falls within this concept and therefore it has to be considered in the light of both Directives 95/46/EC and 2002/58/EC.[15]

What is 'personal data'? Considering that the CTOSE project was developed exclusively for matters concerning 'electronic' evidence, we will first make reference to the environment in which we will find the e-evidence and the personal data connected to it. In this sense, we will connect the concept of personal data with the digital world.

Background: the digital world. An 'information system' can be defined as 'computers and electronic communication networks, as well as computer data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance'.[16]

Computer data can eventually become electronic evidence, because, given a disputed event, 'facts [will] tend to be proved' using this 'information'.[17]

The Internet[18] is a network of computers communicating with each other on the basis of the Internet protocol (TCP/IP).

While for the facility of users, Internet names are commonly represented by textual domain names, the underlying addresses that are used to route data from one host computer to another are numeric.[19] On the Internet, every computer is identified by a single IP address. This numeric system is currently based on numbers that are 32 bits long (IPv4). All Internet applications, both current and future, rely on these addresses. An IP network is based on the transmission of small packets of information. Each packet includes the IP address of the sender and of the recipient.

Internet Access Providers (IAPs) give IPs connection to individuals or organizations (that includes IP address and connectivity). By giving 'connectivity' the IAP guarantees two things: that it will route the packets sent by the client to the final destination and that the packets sent to the client will be routed to him/her as well. Individuals may use a modem (analog modem or DSL—Dynamic System Line) or a terminal adapter (ISDN). In this case the subscriber will receive an IP address for the duration of his/her connection and this address will probably change the next time they dial up. This is called a dynamic IP address. In the case of a connection by ADSL or via video cable, the IP address can be either static or dynamic.

In order to obtain a connection, the individual has to conclude a contract and give his name, address and other personal data. At least for security reasons, the IAPs usually 'log' the date, time, duration and dynamic IP address given to the Internet user in a file.

Internet Service Providers (ISPs) provide services to individuals and companies on the Web. They own or hire a permanent IP connection and use servers permanently connected to the Internet. Classically, they will offer web hosting, access to newsgroups, access to an

```
#Software: Microsoft Internet Information Server 4.0
#Version: 1.0
#Date: 2003-09-11 00:50:32
#Fields: time c-ip cs-method cs-uri-stem sc-status
00:50:32 216.39.48.82 GET /robots.txt 404
00:50:32 216.39.48.82 GET /publications.htm 200
07:27:11 111.111.111.111 GET /Default.htm 304
07:27:11 111.111.111.111 GET /styles/fundp.css 304
07:27:17 111.111.111.111 GET /menu.js 304
07:27:17 111.111.111.111 GET /mm_menu.js 304
07:27:17 111.111.111.111 GET /Cours.htm 200
07:27:17 111.111.111.111 GET /dessins/triangle.gif 404
07:27:25 111.111.111.111 GET /images/valves001.jpg 304
07:27:37 111.111.111.111 GET /TransparentsTitreI.pdf 304
07:27:37 111.111.111.111 GET /dessins/triangle.gif 404
07:28:04 111.111.111.111 GET /dessins/triangle.gif 404
07:28:16 111.111.111.111 GET /epedagogie.htm 304
07:28:16 111.111.111.111 GET /dessins/triangle.gif 404
07:29:50 111.111.111.111 GET /epedagogie.htm 200
07:29:50 111.111.111.111 GET /styles/fundp.css 304
07:29:50 111.111.111.111 GET /menu.js 304
07:29:50 111.111.111.111 GET /mm_menu.js 304
07:29:50 111.111.111.111 GET /images/fundp.gif 304
07:29:50 111.111.111.111 GET /images/Projucit.jpg 304
07:29:50 111.111.111.111 GET /images/cours001.jpg 304
07:29:50 111.111.111.111 GET /images/travaux001.jpg 304
07:29:50 111.111.111.111 GET /images/epedagogie001.jpg 304
07:29:50 111.111.111.111 GET /images/mootcourt001.jpg 304
07:29:50 111.111.111.111 GET /images/valves001.jpg 304
07:29:50 111.111.111.111 GET /images/membres001.jpg 304
07:29:50 111.111.111.111 GET /images/actualites001.jpg 304
07:29:50 111.111.111.111 GET /images/colloques001.jpg 304
07:29:50 111.111.111.111 GET /images/enseignement001.jpg 304
07:29:50 111.111.111.111 GET /images/recherche001.jpg 304
07:29:50 111.111.111.111 GET /images/formations001.jpg 304
07:29:50 111.111.111.111 GET /images/liens001.jpg 304
```

Figure 1. The logfile

FTP (File Transfer Protocol) server and electronic mail. This involves one or more servers using HTTP, NNTP, FTP, SMTP and POP3 protocols.

In the case of HTTP servers a logbook or logfile is systematically created by default and contains some of the data present in the HTTP request header (browser chattering) and the IP address. The logbook is standard practice and is created by each web server.

A logfile may look similar to that shown in Figure 1 (it depends on the web server software and on the configuration).[20]

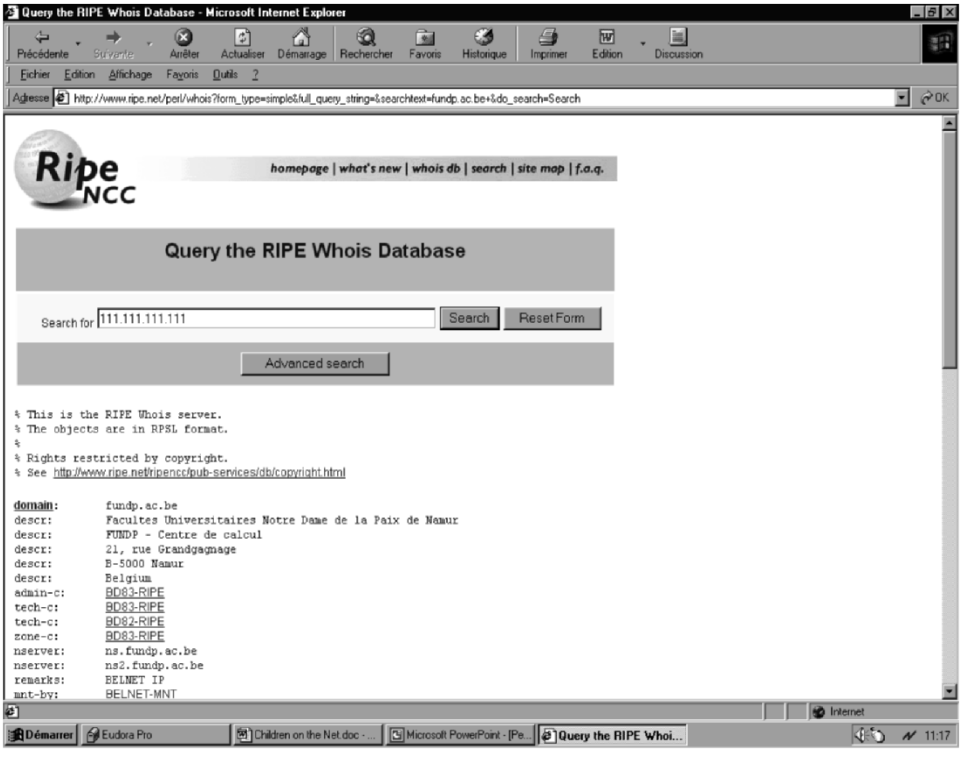

Figure 2. The results obtained when introducing our IP number in the RIPE Whois database

Determining the origin of a packet on the Internet is usually as simple as inspecting the packet and extracting the source address. The ownership of the IP address can then be determined by using the 'Whois' service[21] to interrogate the regional registry databases that describe IP address allocations.[22] This file or 'logbook' can be used, given an electronic disputed event, to 'try' to demonstrate 'who' made 'what' and 'when'.

But, in order to analyse what is the connection of this reality with the Data Protection legislation, we have to know if the data contained in the logfiles can be considered 'personal data', since, if this is the case, Directive 95/46/EC will be applicable, giving place to a series of rights to the data subject and obligations to the data controller.

In Figure 2, we can see the results obtained when introducing our IP number in the RIPE Whois database. Indeed, we can see who has attributed this number and their contact details.

The concept of 'personal data'. Personal data is 'any information relating to an identified or identifiable natural person (data subject). An identifiable person is one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'.[23]

This definition has to be understood jointly with Recital 26 of the Directive: 'Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should

be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; […]'.

When it is technically possible to identify the concerned persons, the data involved has to be considered as 'personal data'.[24] This appreciation has to be made *in concreto*. If the data user alleges that the data is anonymous because it is technically impossible to connect it to other data in order to determine the individual concerned, or that the procedure is excessively costly, he has the burden of proof as regards this possibility and he has to submit evidence to demonstrate that fact.[25]

Can an IP address be identified as 'personal data'? A sole number, can not be considered, as such, 'personal data', unless it could be connected to other information in order to identify a person. If we find a paper on the street, with a series of numbers written, this will not be identified as 'personal data'. If the numbers have the acronym 'GSM' written in front, that could be 'personal data' since it is potentially[26] possible to identify the person to whom this GSM number belongs by requesting the information from the service provider.

As Article 29 ('Working Party') has noted, IAPs and managers of the Local Area Networks (LANs), are potentially able, by using reasonable means, to identify Internet users to whom they have attributed IP addresses as they normally systematically 'log' in a file the date, time, duration and dynamic or static IP address given to the Internet user. They only have to connect this data, with the data of the user/s who have signed the contract for the provision of the service.

System administrators keep a logbook of the HTTP server. Even if they are not normally able to identify directly who is the user behind the IP address (when the user is 'external'), they can identify the IAP, who has given it, by checking in the appropriate registry: RIPE, ARIN or APNIC, etc.[27] By knowing the IAP, it is then, potentially possible to connect the IP address—recorded on the system administrator logfile—to the name and other data of the user/client of the IAP. Here, we have to remember Recital 26 of Directive 95/46/EC, and the reference to '*means likely reasonable* to be used either by the controller or *by any other person* to identify the said person'.

The procedure described above for user identification, does not seem unreasonable, excessively costly or difficult. In this case, the identification would not be done by the controller (the person who has collected the IP address, a website administrator, for instance) but by a third person (the IAP). In principle, a warrant issued by a judge will be necessary to legally make this connection.

In such a case, there is no doubt that one can talk about personal data in the sense of the Directive. Notwithstanding, this data will be 'personal data' as far as the IAP stores the logfiles, through which it is possible to make this connection. As soon as these logfiles are deleted, the IP addresses stored in the logfiles of the web administrators become 'anonymous data'[28] and Directive 95/46/EC is no longer applicable.

In other cases, a third party can get to know the dynamic IP address of a user but not be able to link it to other data concerning this person that would make their identification possible.[29] It is obviously easier to identify Internet users who make use of static IP addresses.

The possibility also exists that the user's IP address can be linked to other personal data (which may or may not be publicly available) that identifies him/her, especially if use is made of invisible processing means to collect additional data on the user (for instance, using cookies containing a unique identifier) or modern data mining systems linked to large data bases containing personally-identifiable data on the Internet users.[30]

Protocol IPv6,[31] the next generation of the Internet, raises a specific concern because of the possibility of the integration of a unique identification number in the IP address.[32] The IP address will not be attributed aleatory, but it will be constituted in part by the serial number of the LAN card in the computer.[33]

As a consequence of this reasoning, data protection legislation, would be applicable to the processing of IP addresses done through logfiles, in those cases where IP addresses[34] can be considered personal data.[35]

Example of IP address considered as personal data. An example of the application of the reasoning described above can be found in the opinion issued by the Belgian Data Protection Authority '*Avis d'initiative concernant la compatibilité de la recherche d'infractions au droit d'auteur commises sur Internet avec les dispositions juridiques protégeant les données à caractère personnel et les télécommunications*'.

In this case, the International Federation of the Phonographic Industry (IFPI) in Belgium had investigated Belgian users who uploaded or downloaded Belgian artists' songs in the Napster Internet site. In order to do so, a representative from IFPI registered himself via a pseudonym to visualize the list of netizens who shared the songs of a Belgian artist. He selected the pseudonym of one of these netizens to download a song. During this process, the representative from the IFPI, used a special software that allowed him to identify the IP address used by the netizen.

Following this, the different IAPs were asked to identify the person who, at the date and hour pointed out, had used the IP address identified by the IFPI, in order to contact them. The IFPI then asked the IAPs to send to the person concerned a warning letter with a request to stop disseminating the songs and to delete them from their hard disk. If this letter is found not be effective, the IFPI would report the crime to the Office of Public Prosecutor (*le parquet*).

The opinion of the Belgian Data Protection Authority analyses therefore the compatibility of investigations against Intellectual Property rights' crimes, committed on the Internet, with the legislation protecting personal data and telecommunications.

This document states, first, that IP addresses can be considered as personal data. It analyses the qualification of this data as 'judicial data', considering that processing is prohibited except given certain conditions regulated by the Belgian law. Second, it analyses the telecommunication framework concerning personal data and the principle of confidentiality.

The opinion of the Belgian Data Protection Authority concludes that an IAP cannot communicate the personal data related to their subscribers to third persons, except in the frame of a judicial procedure. Further, given the legal state-of-the-art, it is up to the judicial authorities, to make all investigations, in order to constitute a list of persons responsible for crimes against intellectual property rights.[36]

This same reasoning was confirmed in the French case 'Metrobus c. Ouvaton'.[37] Here, an ISP that hosted a site where certain illegal activity was conducted, was asked by the plaintiff to identify the creators of this site, since it was causing him damage. The defendant refused to do this without an authorization issued by a judge, because he was constrained by non-disclosure of personal data obligations imposed by the Criminal Code.

Territorial Scope of Application

Article 4 of the Directive describes the connecting factors that will make national laws applicable:[38]

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:
   (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;
   (b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;
   (c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.
2. In the circumstances referred to in paragraph 1(c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

What are the Rights of the Data Subject?

The data subject has the following rights (which suppose correlative obligations for the data controller *vis-à-vis* them):

(1) To receive certain information before the collection of personal data.[39]

The controller has to inform the data subject about:

- his identity,
- the purposes of the processing for which the data are intended,
- the recipients or categories of recipients of the data (if appropriate),
- the existence of the right of access to and the right to rectify the data concerning him, etc.

The controller has to inform, at the time of the collection of the data, and in the case when the data has not been obtained directly from the data subject. In the case of the Internet, this obligation is normally fulfilled through a Privacy Policy. A link to the policy must be present in every page. Information of clickstream data collection, *formulaires* where personal data is required (the character—mandatory or not—of the provision of these data), use of e-mail, etc., has to be given as well as the purposes for this processing.

(2) Right of access.

Member States shall guarantee every data subject the right to obtain from the controller:

Without constraint at reasonable intervals and without excessive delay or expense:

—confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,

—communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,

—knowledge of the logic involved in any automatic processing of data concerning him at least in the case of automated individual decisions.[40]

The exercise of the right of access, however, does not proceed in the case of an indirectly identifiable data subject, since, the data controller can not identify him by his own (see above).

The situation would be different, if the data subject has suspicions about whether the data controller would have combined data from different sources, making possible his identification. In this second hypothesis, particular attention has to be paid, to Article 15 of the Directive, in the case automated individual decisions be taken.[41]

(3) Right of rectification, erasure or blocking of data the processing of which does not comply with the provisions of the Directive.[42]

This is a consequence of the right of access, and allows the data subject to control the regularity, legality, and accuracy of the data processed about him.

(4) Right not to be subject to automated individual decisions.[43]

What are the Obligations of the Data Controller?

Conditions for Processing Personal Data

Controllers must respect five basic principles relating to the quality of data. Personal data must be:

(1) Processed fairly and lawfully.[44]

'Fair' processing requires transparency. An individual's personal data cannot be processed for any hidden or secret reason. The concretization of this principle can be seen in the obligation to inform the data subject about the identity of the controller, the purposes of the processing, etc.

'Lawful' processing requires compliance with national provisions. For example, disclosure may be lawful only when authorized by the national law, for example, in the case of preservation orders related to traffic data.

(2) Collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.[45]

(3) Adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.[46]

This concept is strictly connected to and conditioned by the purpose of the processing activity. It will determine the content and the amount of data that can be collected. So, in case that the system administrator, declares in the Privacy Policy, that he/she collects clickstream data for the normal administration of the site (eg to know what are the most visited pages), he/she will not be authorized to connect this data to other personal data (eg data-mining of IP addresses) in order to know more about the characteristics of the visitors.

(4) Accurate, and when necessary, kept up to date.[47]

Data are inaccurate, if they contradict objective truth or findings, or if they are incomplete. The mere fact of storing IP addresses in logfiles does not give place for inaccuracies. Attention to this principle should be given, if further processing is done with this data that could incur lack of precision or need updating.

(5) Kept in a form that permits identification of data subjects for no longer than necessary for the purposes for which the data were collected or for which they are further processed.[48]

In general, the necessity has to be determined in connection with the purpose. Nevertheless, it can also be determined by law, as we will see hereinafter, for example, in the case of traffic data conservation and/or retention.

What Makes Data Processing Legitimate?

Personal data may be processed only if:

(1) The data subject has unambiguously given his consent.[49]

The Directive defines the 'consent of the data subject' as 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed'.[50]

A 'freely given' consent means the absence of any kind of pressure. 'Specific' means that the consent for the processing of certain data does not authorize the controller to process data for other purposes without obtaining the consent again. 'Informed' means that the data subject is aware of the processing activities that his data will be subject to, as the controller has given proper details about it.

On the Internet, the consent of a data subject can be gathered through proper information given, for example, in the form of privacy policies. A visible hyperlink not only in the home page, but on every page, will bring the visitor to a description page containing the policy. This statement will indicate to the surfer that continuing the visit of this website involves the consent to the processing described (of course this processing has to be lawful and legitimate as mentioned above). However, this way of obtaining consent, can be questioned in what concerns the 'informed' characteristic, mainly in those cases where the privacy policy is mentioned in small letters, at the end of the website, hidden by misleading terms such as 'legal', 'policies', etc. To conclude that the consent has been gathered in an 'informed' way in those cases, the visitor has to be given a conspicuous possibility to read the privacy policy.

(2) processing is necessary for the performance of a contract to which the data subject is party;[51] [or]

In the instance of IAPs, logging of data can be justified for the fulfilment of contractual obligations (this is one of the justifications, then we will have the use of exceptions under Article 13.1 of Directive 95/46/EC and Article 15.1 of Directive 2002/58/EC, see below).

As a general principle, the controller should be able to prove the 'necessity' of the processing for the conclusion or execution of the contract.

In the case of an e-commerce operation, the data required should be those needed for deliverance of the product. If the transaction deals with the provision of a service, only those data necessary for the controller to comply with the obligation, may be asked for in order to be justified under this premise.

(3) Processing is necessary for compliance with a legal obligation to which the controller is subject;[52] [or]

This is the case of IAPs who are obliged by law to store traffic data for certain amount of time (retention and preservation).

(4) Processing is necessary to protect the vital interests of the data subject;[53] [or]

This condition has, *prima facie*, no relevance for the scope of CTOSE.

(5) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller or in a third party to whom the data are disclosed;[54] [or]

This regulation is applicable to processing activities carried out mainly in the public sector. For instance, this is the case of processing made by the police, judicial power, etc.

(6) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject that require protection under Article 1.[55]

This regulation thus provides the possibility for the controller to process personal data when he/she or a third party, has a 'legitimate interest' to do so. To maintain the balanced required by the Directive and guarantee effective competition, Member States have to determine the circumstances in which personal data can be processed in this context.[56] This is a very useful tool for the business sector.

The balance will be made first by the controller. If the data subject objects it, and in the case that they do not reach an agreement, the case would be submitted to the National Data Protection Authority for interpretation, and in the last case, to a judge.

Other Obligations

Further to the obligations already described, the data controller must implement security measures against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular, where the processing involves the transmission of data over a network.[57] They also must notify[58] the national data protection authority before any processing operation (Member States may simplify or exempt data controllers from this obligation given certain circumstances. System administrators have to evaluate which kind of processing they make and confront them with the requirements and exceptions foreseen in the applicable national law as regards the obligation of notification).

Exceptions and Restrictions to the Rights and Obligations

Privacy and the protection of personal data are not absolute rights. They can be limited when a balance is necessary to safeguard other important public policy interests, such as the case of the fight against crime. As a consequence, both Directives 95/46/EC[59] and 2002/58/EC[60] describe the requisites that should be respected when limiting the protected rights. These rules follow the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms[61] and the doctrine of the European Court of Human Rights.

For instance, Directive 95/46/EC stipulates that:

> Member States may adopt legislative measures to restrict the scope of the obligations and rights (*principle of legitimate purpose, information to the data subject, right of access*[62]) when such a measure constitutes a necessary measure to safeguard:
>
> (a) national security;
> (b) defence;

(c) public security;
(d) the prevention, investigation, detection and prosecution of criminal offences, or breaches of ethic for regulated professions;
(e) an important economic or financial interest of a Member State or of the European Union, […];
(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
(g) the protection of the data subject or of the rights and freedoms of others.

Obligation to Store Traffic Data[63]

An example of an exemption to certain obligations contained in personal data protection rules is the regulation concerning the retention of traffic data. Within CTOSE, consideration must be given to the regulation as regards traffic data storage, because this data would be necessary to make an eventual link between an IP address and a given user.

> 'Traffic data' is defined as 'any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof'.[64]

Directive 2002/58/EC foresees[65] that interception or surveillance of communications and the related traffic data is prohibited, except when legally authorized in accordance with article 15.1. We have to remember that it is a legal principle to interpret 'exceptions' restrictively.

The principle is that traffic data must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication, here again, without prejudice to Article 15.1.

We have to point out that both Directives 95/46/EC and 2002/58/EC are instruments regulating the protection of fundamental rights, so they determine the conditions to follow when restricting them, but not the restrictions themselves. It is for other kind of Conventions or laws to do so.

This is the case of the Council of Europe Convention on Cyber-crime which determines that Parties shall adopt legislative measures to order a person to preserve and maintain specified computer data, including traffic data, for a period of time as long as necessary, up to a maximum of 90 days.

It is important to distinguish between 'retention' and 'preservation'. The first one is made *ex ante*, which means systematically and during a certain period. It includes traffic data but not content data. The second one is made *ex post*, which is after a disputed event has happened, and includes content data. This last notion is the one used in the Cyber-crime Convention. It involves 'freezing' the data already stored, through a 'preservation order' (warrant). Member States have no harmonized regulations in this arena, so the study of national laws is indispensable.

Suspicious Phase and Investigation Phase

In these phases the web administrator and the IAP are subject to the same obligations as in the Running phase. However, the stipulations of Article 13.1 of Directive 95/46/EC and Article 15.1 of Directive 2002/58/EC are relevant in what concerns the restrictions of the rights and obligations provided in those texts (see above).

This implies, for instance, that the request to the IAP to connect the IP address found in the logfile of a web administrator involved in a cyber-attack with the personal data necessary to identify the user (client of the IAP), will only be legally done with a warrant issued by a judge. That will exempt the data controller of his obligation of confidentiality. The same can be said as regards traffic data. The principle is to erase it or make it anonymous when it is no longer needed for the purpose of the transmission of a communication, but, being that this data is necessary in the fight against cyber-crime to identify wrongdoers, many countries have adopted legislation limiting this obligation.

Applicable Legislation in Criminal Cases as Regards Personal Data Protection

Directive 95/46/EC is a first pillar instrument regulating the internal market. When it was transposed to national systems, many countries extended the application of the national law to their whole legal system, because of their respect for the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data No. 108, which is indeed applicable to the whole legal system. That means that the scope of the national laws is irrespective of the scope of the Directive, being broader and covering the processing of personal data even in those areas excluded from Directive 95/46/EC, such as criminal law.

In the context of the Council of Europe instruments, consideration will be taken of the Recommendation No. R (87) 15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector. This is not a mandatory instrument but it gives guidelines to governments on this issue.

In the EU context, the Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention) establishes a European Police Office, which liases with national units in each Member State. It aims to improve the effectiveness and cooperation of the competent authorities in the Member States combating serious forms of international crime. It regulates a computerized system of collected information and the applicable data protection rules.

In the future, the Proposal for a Council Framework Decision on attacks against information systems[66] and its relation with privacy legislation will have to be considered, as well as the reference it makes to Convention 108. The objectives of the (Draft) Council Framework Decision are to approximate criminal law in the area of attacks against systems and to ensure the greatest possible police and judicial co-operation in the area of criminal offences related to attacks against information systems. Moreover, this proposal contributes to the efforts of the EU in the fight against organized crime and terrorism. The legal basis of this Framework Decision is Title VI of the European Union Treaty (police and judicial co-operation in criminal matters, third pillar issues).

What are the Risks for Violation of Data Protection Rules?

We can identify three risks for violation of data protection rules in the context of the CTOSE project: civil liability, criminal liability and inadmissibility of e-evidence.

Civil Liability

Every person has the right to a judicial remedy for any breach of the rights guaranteed to him by the national personal data protection law applicable to the processing in question.[67]

Then, if the data subject suffers damage as a result of unlawful processing of his/her personal data, he/she is entitled to receive compensation from the controller.[68] 'The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event rise to the damage.'[69] Grimalt Servera considers that this regime creates a liability without fault system.[70]

Criminal Liability

The punishment for violations to the national laws transposing the Directive will be different in the Member States, because this area of law is not harmonized within the EU (procedural law, criminal law).[71]

Many European personal data protection laws penalize the perpetrators of violation of data protection principles with fines and/or imprisonment. In Table 1 we can see some examples of criminal sanctions for violation to data protection obligations.

There has been a recent case in France where a person was condemned by a Criminal Court of Appeal because of non-declaration of personal data processing to the CNIL, an infraction that is penalized by Articles 226-16 and 226-31 of the French Criminal Code, and Articles 16 and 41 of the Act 78-16 of 6.1.1978.[72]

Inadmissibility of E-evidence

In a vertical relation (State–citizen) strict consideration to Article 8.2 of the European Convention for the Protection of Human Rights and Fundamental Freedoms ('EHRC') must be made. If evidence has been gathered by Law Enforcement Agents (LEA) limiting an individual's privacy, such evidence collection must be both 'in accordance with the law' and (that law must be) 'necessary in a democratic society' as set forth by the second paragraph of Article 8 (EHRC) to be admissible. Otherwise the evidence risks being declared inadmissible. This has been confirmed on many occasions by the European Human Right Court: 'The expression "in accordance with the law" requires, firstly, that the impugned measure should have some basis in domestic law; secondly, it refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must moreover be able to foresee its consequences for him, and that it is compatible with the rule of law […] The Court notes that Regulation of Investigatory Powers Act 2000 contains provisions concerning covert surveillance on police premises. However, at the relevant time, there existed no statutory system to regulate the use of covert listening devices by the police on their own premises. The interference was not therefore "in accordance with the law" as required by the second paragraph of Article 8 and there has been a violation of this provision. In these circumstances, an examination of the necessity of the interference is no longer required.'[73]

In a horizontal relation (e.g. between private entities) the parameters of Article 8 (EHRC) have to be respected as well. In the Belgian labour dismissal case 'Depresseux c. s.a. Creaspace & Masereel', the judge rejected the employer's claim since the evidence was gathered in violation of Article 8 (EHRC) and Article 29 of the Belgian Constitution. In this case, the employer discovered, by secretly inspecting the employee's computer-control of e-mails, that his employee was conducting a parallel activity, unrelated to his job. The Court considered that employees have, even during working time, the right to privacy, which implies the right to secrecy of correspondence. By consequence, evidence collected in

Table 1 Examples of criminal sanctions for violation to data protection obligations

	EU (article in the Directive)	Belgium	Italy	France	UK
Information	10, 11	Fine; Art. 39.4		Fine and imprisonment; Art. 226-16 Criminal Code	Section 40 and 47 of the UK Act
Access	12	Fine; Art. 39.5		Fine and imprisonment; Art. 226-16 Criminal Code	Section 47 of the Act (see principle n. 6 of the Schedule I, Part I.)
Notification	18, 19	Fine; Art. 39.7	Fine (lack of or incomplete notification); Art. 34. Imprisonment (Misrepresentation); Art. 37-bis.	Fine and imprisonment; Art. 226-16 Criminal Code	
Security	17	Fine; Art. 38 (only affecting the duty of Art. 16.1: oblig. To chose a subcontractor who provides for sufficient guaratees concerning security measures)	Fine or imprisonment; Art. 36.	Fine and imprisonment; Art. 226-17 Criminal Code	Section 47 of the Act. (see principle n. 7 of the Schedule I, Part I)

violation of those rights can not be accepted.[74] Notwithstanding, the judge did not consider the violation to the Belgian law on personal data protection, in the specific sense.

However, it must be assessed to what extent the use of electronic evidence, including e-traces, collected and processed in violation of personal data protection legislation can undermine the validity of this evidence. The answer to this question will suppose a thorough study of national case law, as well as the jurisprudence of the European Court of Human Rights. We cannot make general statements since the admissibility or inadmissibility of the evidence will vary considering the very circumstances of the case and the national procedural system. As far as we know, there has been little decisive case law analysing the validity of electronic evidence gathered in violation of data protection rules in Europe.

The European Charter of Fundamental Rights, which includes the fundamental right to data protection can also be considered in this realm. Even if this instrument is not yet

binding, we may wonder what will be its influence in the admissibility of evidence gathered in violation of the very principles expressed in Article 8 (e.g. fair processing, for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law, right of access and rectification).

One could imagine the case of a system administrator who keeps the logfiles of the HTTP server and other data collected via his e-commerce site, but who had not notified the national DPA of this processing activity, and had not informed visitors about his identity, the purposes of the processing for which the data are intended, and the existence of the right of access to and the right to rectify the data concerning him.[75] The data he collected via the e-commerce site was notably excessive in relation with the purpose of delivering a product. He used these data to make profiles of the consumers and send them advertising via different channels. He suffers an attack and, using the logfile he can identify the IP address of the attacker. Considering that the administrator had business problems with certain customers who were very disappointed with his products, he suspects that one of them could be the wrong doer. In several cases, the data of the logfile can be connected (using a data mining technique) with the data of the e-commerce transactions. The system administrator identifies the attacker, files a criminal complaint and presents this evidence. Can we infer that there is a risk of inadmissibility of this evidence because of the violation of the obligations imposed by the data protection law? We cannot give a definite answer because, as we have already said, any decision will be based on the specific facts of the case and national procedural law.

However, here there could be a certain risk of inadmissibility because the obligations imposed by the data protection law to the data controller have not been respected, and the collection of the evidence was made in a state of violation to the law. We could consider, nevertheless, a Belgian case law that states that evidence that has been collected illegally can not be used as such but may be used as the basis for the accusation ('*la preuve d'une infraction diffère de la communication d'un délit [en ce qu'] une communication ne peut être tenue pour inexistante*')[76]. Further research would be necessary on procedural law issues and on a national basis to be able to give a more accurate answer.

Even if this case is quite unlikely to happen in reality (hackers are not as *naive* as the one in the example), it is important to visualize that specific problems can arise from the lack of complaint with the positive obligations derived from the data protection legislation, which in EU countries is considered to be of public order.

We can wonder then, what would happen if having obtained the IP address of the attacker from his logfile (which was kept for security reasons, for statistic purposes and not for matching with other data) the system administrator files a complaint and the LEA proceeds with a warrant to request the IAP (after having identified him using the Whois service) to connect this IP number with the data of the user to whom this IP address was attributed.

In this second hypothesis, the risk of inadmissibility is reduced. First of all, when the data subject can only be identified indirectly, certain obligations like notification, information, or access, are reduced, and even, in certain circumstances, not directly applicable (to be checked at national level). Second, considering that the LEA intervened with a warrant, the risks for the rights to privacy and personal data are reduced also, since, a judge has evaluated that the identification be made in accordance with the law.

Concluding Remarks

Despite this very general and brief approach to the relation between personal data protection legislation and electronic evidence handling, we could highlight the obligations that should be taken into account by the data controllers and the legal risks that could exist, eventually, if personal data is not legally processed.

After our experience in the CTOSE project we realize that non-lawyers, who normally handle electronic evidence, tend to identify privacy and personal data protection with confidentiality and security measures. This derives from the false belief that by complying with the last two obligations they respect the law. However, all the other obligations ruled in the Directive have to be taken into account by system administrators and other people intervening in activities dealing with electronic evidence handling. These obligations should not be neglected when designing any tool or methodology aimed at handling evidence or fighting against illegal on-line activities (e.g. intrusion detection systems).

Considering that procedural law is not harmonized at EU level, further research would be encouraged to better determine the intrinsic interaction between the violation of positive data protection obligations and the inadmissibility of electronic evidence obtained as a consequence of that violation.

Notes and References

1 This paper has been written in the context of the CTOSE project (IST programme), and it is an adaptation and briefing of Deliverable 3.2 'Privacy and personal data protection constraints'. It was the basis for the presentation at the CTOSE Conference. This paper, however, is solely the responsibility of the author and does not represent the opinion of the other contributors to the CTOSE project or of the European Community. I am particularly grateful to Dr Cécile de Terwangne, Professor at the Faculty of Law, University of Namur and Director of Research at the CRID, Jean-Marc Dinant, computer scientist and Director of research at the CRID, and Jan Dhont, Solicitor and researcher at the CRID, for their valuable comments during the drafting of the CTOSE Deliverable.

2 CTOSE Project results, available at: http://www.ctose.org/ResultsPaperv6.pdf.

3 E Jauchen 'Tratado de la prueba en material penal' *Rubinzal-Culzoni Editores*, Buenos Aires, 2002; M Hairabedian 'Eficacia de la prueba ilícita y sus derivadas en el proceso penal' *Ad-Hoc*, Buenos Aires, 2002; Y Poullet and O Leroux 'En marge de l'affaire GAIA: De la recevabilité de la preuve pénale et du respect de la vien privée' *Revue Générale de Droit Civil Belge*, Vol 3, 2003, pp 163–176.

4 See: J M Dinant 'Le visiteur visité' *Lex Electronica*, 2001, available at: http://www.lex-electronica.org/articles/v6-2/dinant.htm, last visited 18 April 2002; J Reidenberg 'Resolving conflicting international data privacy rules in cyberspace' *Stanford Law Review*, Vol 52, 2000, pp 1315–1376; C Ducourtieux and S. Foucart 'Les profileurs du Net traquent les internautes à leur insu' *Le Monde*, 10 May 2002, p 20.

5 Specially in the SMEs sector, even the data controller (web site administrator) may be unaware about the fact that he/she is collecting personal data, since logfiles are created by default (see the concept of 'personal data' and 'data controller').

6 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23 November 1995. Hereinafter: 'the Directive'.

7 Further information about the Process Model 'phases' can be found at http://www.ctose.org.

8 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31 July 2002.

9 Article 1.2 of Directive 2002/58/EC.
10 Article 2(d) of Directive 95/46/EC.
11 Article 2(e) of Directive 95/46/EC.
12 Article 16 of Directive 95/46/EC.
13 Article 17.3 of directive 95/46/EC.
14 Article 2(b) of Directive 95/46/EC.
15 Article 29 WP 'Privacy on the internet—an integrated EU approach to on-line data protection' 21 November 2000, WP37, pp 22–23, (adaptation done by us). Available at: http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp37en.pdf.
16 Article 2 (d). COM (2002) 173 final.
17 A Kean *The Modern Law of Evidence* 5th edn. Butterworths, London, 2000, p 1.
18 To describe the technical aspects we follow the document 'Privacy on the internet—an integrated EU approach to on-line data protection', 21 November 2000, WP37, elaborated by the Article 29 WP (*op cit*, note 15) to be given to the fact that technical aspects have been simplified in this paper. See also: A. Ambrosini *La tutela del nome di dominio*, Edizioni Simone, Napoli, 2002, pp 15–32.
19 Communication from the Commission to the Council and the European Parliament 'The Organisation and Management of the Internet. International and European Policy Issues 1998–2000', Brussels, 11 April 2000, COM(2000) 202 final. See mainly pp 19 and 20 of this document (Data protection aspects: registration and Whois data; Domain name registration data flows; Transparency and access to data.), as well as p 32 (Domain name registration data and data protection—Whois).
20 As we can see, it does not only contain the IP address of the person who has requested access to a certain website, but also, when, what did he want to see and whether the access was given or not. So, we see that we can even infer the content of what he has seen (in this example the IP addresses have been changed).
21 RIPE (Réseaux IP Européens, http://www.ripe.net), ARIN (American Registry for Internet Numbers, http://www.arin.net/), APNIC (Asia Pacific Network Information Centre, http://www.apnic.net/), etc. For an overview on privacy and data protection implications of Whois database, see Electronic Privacy Information Center (EPIC) 'Whois', available at: http://www.epic.org/privacy/whois, last visited 30 April 2003. International Working Group on Data Protection in Telecommunications 'Common position on privacy and data protection aspects of the registration of domain names on the Internet', adopted at the 27th Meeting of the Working Group on 4–5 May 2000 in Rethymmon, Crete, available at: http://www.datenschutz-berlin.de/doc/int/iwgdpt/dns_en.htm, last visited 30 April 2003. European Commission, Internal Market DG, Data Protection 'Contribution of the European Commission to the general discussion on the Whois database raised by the Reports produced by the ICANN Whois Task Force', available at: http://www.dnso.org/dnso/notes/ec-comments-whois-22jan03.pdf.
22 LINX Content regulation Committee 'LINX best current practice—traceability', version 1.0, last modified 18 May 1999, available at: http://www.linx.net/noncore.bcp/traceability-bcp.html, last visited 12 July 2002.
23 Article 2(a) of the Directive.
24 This concept has, however, been interpreted differently in the UK. See for instance: *Durant* v *FSA* [2003] EWCA Civ 1746.
25 See M H Boulanger, C de Terwangne, T Leonard, S Louveaux, D Moreau and Y poullet 'La Protection des données à caractère personnel en Droit Communautaire' *Journal des Tribunaux Droit Européen*, June 1997, p 1 and ss.
26 We use the word 'potentially' because may be the search will not give a correct result, since the telephone could have been stolen, so we will find the owner but not the user, or the acronym 'GSM' meant something else than 'Global System for Mobile communications'.
27 The InterNIC is an integrated network information centre and Whois service for the existing gTLDs, .COM, .NET and .ORG. Similar InterNIC and Whois services are provided by the country code Registries and the regional IP Registries, e.g. RIPE.

28 The only hypothesis in which the qualification of 'personal data' would remain is the case when the web administrator has collected personal data from different sources being able to identify the user of a given IP address.
29 Due to proxy servers, anonimizers, etc.
30 Article 29 WP, *op cit*, note 15.
31 See 'Internet Protocol, Version 6 (IPv6) specification' *Network Working Group*, December 1998. Available at: http://www.arin.net/library/rfc.rfc2460.txt, last visited 22 June 2002.
32 J-M Dinant 'The arrival of the new Internet network numbering system IPv6 and its major risks to data protection' ECLIP (*Electronic Commerce Legal Issues Platform*), IST Project 1999-12278. Available at: http://www.eclip.org, last visited 8 May 2002. Article 29 WP Opinion 2/2002 on 'The use of unique identifiers in telecommunication terminal equipments: the example of IPv6', 30 May 2002, WP58. Available at: http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp58en.pdf.
33 See Ducourtieux and Foucart, *op cit*, note 4, quoting Jean-Marc Dinant.
34 The Belgian Data Protection Authority has issued an interpretative document in which it specifies different categories of data. Under point A.2 it includes 'Données d'identification électronique: addresses IP, cookies, moments des connexion, …'. See 'Lexique No. 3'. Available at: http://www.privacy.fgov.be/declarations/lexique3.htm, last visited 11 July 2002.
35 It will be a question of analysis considering, for example, the variables described above (e.g. deletion of the IAP logfile).
36 *Avis d'initiative concernant la compatibilité de la recherche d'infractions au droit d'auteur commises sur Internet avec les dispositions juridiques protégeant les données à caractère personnel et les télécommunications,* Numéro de rôle 44/2001. See also G Rue and F. de Patoul 'L'affaire Napster ou le difficile équilibre entre le droit d'auteur et le respect de la vie privée' *Revue Ubiquité. Dr. tech. Info*, No 12, June 2002.
37 See the case 'Metrobus c. Ouvaton', TGI Paris, référé, 1 December 2003.
38 We will not develop the applicable law implications in this paper.
39 Articles 11 and 12 of Directive 95/46/EC.
40 Article 12(a) of Directive 95/46/EC.
41 L Bygrave 'Minding the machine: Article 15 of the EC Data Protection Directive and Automated Profiling' *Computer Law & Security Report*, Vol 17, pp 17–24, 2001.
42 Article 12(b) and (c) of Directive 95/46/EC.
43 Article 15.1 of Directive 95/46/EC.
44 Article 6(1)a of Directive 95/46/EC.
45 Article 6(1)b of Directive 95/46/EC.
46 Article 6(1)c of Directive 95/46/EC.
47 Article 6(1)d of Directive 95/46/EC.
48 Article 6.1.e) of Directive 95/46/EC.
49 Article 7(a) of Directive 95/46/EC.
50 Article 2(h) of Directive 95/46/EC.
51 Article 7(b) of Directive 95/46/EC.
52 Article 7(c) of Directive 95/46/EC.
53 Article 7(d) of Directive 95/46/EC.
54 Article 7(e) of Directive 95/46/EC.
55 Article 7(f) of Directive 95/46/EC.
56 Recital 30 of Directive 95/46/EC.
57 Article 17 of Directive 95/46/EC
58 Article 18 of Directive 95/46/EC
59 Article 13.1 of Directive 95/46/EC. See also Recitals 43, 44, and 45 of the Directive.
60 Article 15.1 of Directive 2002/58/EC.
61 Article 8.2: 'There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the

interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'.

62 Words in italics added by us.

63 See S Louveaux and M V Pérez Asinari 'New European Directive 2002/58 on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector—some initial remarks' *Computers and Telecommunications Law Review*, Vol 9, No 5. M V Perez Asinari 'La regulación de los datos de tráfico en la Unión Europea. ¿Entre la seguridad y los derechos fundamentales?' Lexis Nexis, Jurisprudencia Argentina, Vol 4, pp 49–59, 2004.

64 Article 2(b) of Directive 2002/58/EC.

65 Article 5.1 of Directive 2002/58/EC.

66 Proposal for a Council Framework Decision on attacks against information systems, Brussels, 19 April 2002, COM (2002) 173 final.

67 Article 22 of Directive 95/46/EC.

68 For a complete study on data protection and civil liability issues see P Grimalt Servera 'La responsabilidad civil en el tratamiento automatizado de datos personales' PhD thesis, Editorial Comares, Granada, 1999.

69 Article 23.2 of directive 95/46/EC.

70 '[Se] instituye un régimen de responsabilidad basado en el incumplimiento del estatuto jurídico del responsable del fichero, alejado de cualquier connotación de culpa; es decir, establece un régimen de responsabilidad objetiva por incumplimiento normativo […].' (Grimalt Servera, *op cit*, note 69, p 369).

71 Article 24 of Directive 95/46/EC.

72 Tribunal de Grande Instance Villefranche sur Soane, 'Roger G.', 18 February 2003. In this case, an 'internaut' had created a website consecrated to the fight against the sects where the name of a physical person was mentioned. The mentioned person, considering himself a victim, brought a criminal lawsuit against the creator of the website. The defendant alleged that he had not notified the CNIL since he did not know about this obligation and since any information had been received neither from the media nor from the IAP. However, the Court rejected those arguments and condemned him to pay a fine. See 'Un internaute condamné pour absence de déclaration de son site à la CNIL' *Forum des droits sur l'internet* 26 March 2003, available at: http://www.foruminternet.org/tete/actualites/lire.phtml?id = 527&print = 1, last visited 28 April 2003.

73 European Court of Human Rights, Case of *P.G. and J.H.* v *The United Kingdom*, Application No. 44787/98, Judgment, Strasbourg, 25 September 2001.

74 Depresseux c. s.a. Creaspace & Masereel, Trib. Trab. Verviers (1re ch.), 20 March 2002.

75 We assume that the system administrator is *in casu* a data controller.

76 INUSOP, Cass., 5 April 1996, Arr. Cass., 1996, No. 111.